PELAPORAN INTRUSI PADA WEB SERVER BERBASIS SMS GATEWAY

Agus Priyo Utomo[1], Isbat Uzzin Nadhori[2]
Mahasiswa Jurusan Teknik Komputer dan Jaringan[1], dan Dosen Pembimbing[2]
Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember
Kampus PENS-ITS Keputih Sukolilo Surabaya 60111
Telp. 031 – 59472080, 031 – 5946114, Fax : 031 – 5946114
E-mail : sawer@student.eepis-its.edu

Makalah Proyek Akhir

ABSTRAK

Suatu server yang terhubung dengan internet selalu rawan dengan serangan dan exploitasi dari para hacker ataupun attacker. fakta ini dapat dilihat dari banyaknya aksi para hacker/attacker di dunia internet dalam melakukan serangan pada server - server website. didukung juga dengan banyaknya tutorial - tutorial yang tersebar diinternet yang memicu para pemula untuk mencoba mengeksploitasi website - website yang ada. banyaknya teknik hacking memberikan kesempatan kepada attacker untuk mencoba berbagai teknik tersebut. Dengan membuat pelaporan intrusi pada web server berbasis sms gateway, maka administrator tidak perlu lagi harus berada di depan mesin server atau memeriksa log file pada console di LINUX. Tugas tersebut telah digantikan oleh program perl yang kemudian ditampilkan pada website report. Perintah - perintah program yang memisahkan log file mod_security di server dengan bantuan pemrograman perl yang dikombinasikan dengan regural expresion agar pelaporan pada website mudah dimengerti. Dengan sistem pelaporan intrusi berbasis sms gateway ini diharapkan mampu memudahkan dan mempercepat kinerja Administrator Jaringan untuk menindak lanjuti intrusi – intrusi yang masuk di server.

Kata Kunci : Mod_Security, Regural Expresion, Perl, Security Server, Web Aplication Firewall.

ABSTRACT

a server connected to the Internet is always vulnerable to attacks and exploitation by hackers or attackers. This fact can be seen from the many actions of the hacker / attacker in the world of the Internet in an attack on the servers site. supported also by the number of tutorials that spread the internet that trigger the beginner to try to exploit the website - the website available. the number of hacking techniques provide the opportunity for the attacker to try different techniques. By making the reporting of intrusions on the web-based sms gateway server, so administrators no longer need to be in front of the server machine, or check the log file on the LINUX console. The task has been replaced by a perl program which is then displayed on the website report. The command that separate programs mod_security log file on the server with the help of perl programming combined with regural expresion for reporting on the website easy to understand. With the reporting system based sms gateway intrusion is expected to facilitate and accelerate the performance of Network Administrator for follow-up intrusions that entered on the server.

Keyword : Mod_Security, Regural Expresion, Perl, Security Server, Web Aplication Firewall.

BAB 1
PENDAHULUAN

1.1 LATAR BELAKANG

Berkembangnya teknologi informasi khususnya jaringan komputer dan layanan-layanannya di satu sisi mempermudah pekerjaan - pekerjaan manusia sehari-hari, akan tetapi di sisi lain timbul masalah yang sangat serius, yakni faktor keamanannya. Di satu sisi manusia sudah sangat tergantung dengan sistem informasi, akan tetapi di sisi lain statistik insiden keamanan meningkat tajam. Hal ini secara umum terjadi karena kepedulian terhadap keamanan sistem informasi masih sangat kurang. Untuk mencegah insiden keamanan perlu dilakukan langkah-langkah preventif baik teknis ataupun non teknis.

Sistem pertahanan sistem terhadap aktivitas gangguan yang ada saat ini umumnya dilakukan secara manual oleh administrator. Hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan administrator dalam merespon gangguan yang terjadi.

Apabila gangguan tersebut telah berhasil membuat jaringan mengalami malfungsi, administrator tidak dapat lagi mengakses sistem secara remote. Sehingga administrator tidak dapat melakukan pemulihan sistem dengan cepat.

Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Sistem deteksi penyusupan jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem yang ada pada saat ini tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang mengadministrasi sistemnya. Hal ini merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis.

Pada penelitian ini akan didesain dan diimplementasikan suatu sistem deteksi penyusupan jaringan yang memiliki kemampuan untuk mendeteksi adanya aktivitas jaringan yang mencurigakan, melakukan tindakan penanggulangan serangan lebih lanjut, serta mampu berinteraksi dengan administrator menggunakan media SMS (Short Message Service) satu arah.

1.2 PERMASALAHAN

Permasalahan yang ditangani dalam pembuatan aplikasi pendeteksian intrusi pada webserver berbasis sms gateway ini antara lain adalah penyediaan sebuah sistem security server yang berfungsi untuk memberikan informasi kepada administrator bahwa ada tindakan - tindakan dari pihak luar (attacker) untuk berusaha masuk kedalam system.

1.3 TUJUAN

Adapun tujuan dari pembuatan tugas akhir ini dapat di bedakan menjadi tujuan umum dan tujuuan khusus, yaitu :

1.3.1 TUJUAN UMUM

Untuk memenuhi persyaratan akademis menyelesaikan studi pada jurusan Teknik Komputer dan Jaringan di Politeknik Elektronika Negeri Surabaya.

1.3.2 TUJUAN KHUSUS

Tujuan proyek akhir ini adalah membangun system pelaporan intrusi yang masuk pada sebuah server sebagai alert kepada Administrator agar dengan cepat menditeksi serangan.

1.4 BATASAN MASALAH

Pada penyelesaian tugas akhir ini terdapat beberapa batasan masalah yang dikaitkan dengan pembuatan pelaporan intrusi pada webserver ini, antara lain :

a. Operating sistem yang digunakan adalah Ubuntu / Linux.
b. Software detection intrusin adalah mod_security.
c. Pemrogaman perl yang di integrasikan dengan regular expresion guna memisahkan isi dari log mod_security.
d. Gammu guna untuk mengirimkan sms / sms gateway
e. Intrusi yang difilter hanya SQL Injection

BAB 2
TEORI PENUNJANG

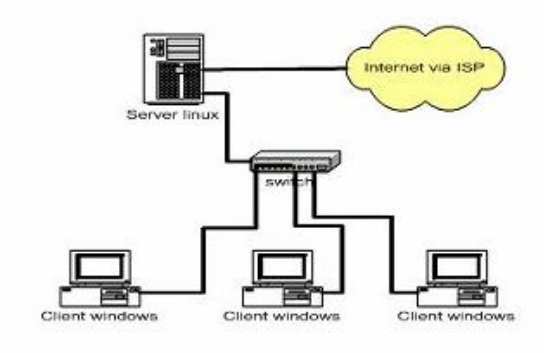
2.1 UMUM

Internet merupakan jaringan komputer yang terbentuk oleh komputer-komputer di seluruh dunia. Komputer-komputer tersebut dapat saling berhubungan atau berkomunikasi antara satu dan yang lainnya meskipun beda platform maupun system operasi. Hal ini dimungkinkan karena adanaya protocol jaringan yang disebut dengan TCP/IP. TCP/IP merupakan protocol jaringan paling utama saat ini.

Protokol ini pertama kali dipergunakan oleh militer Amerika Serikat. Pada perkembangannya protocol ini kemudian menjadi protocol jaringan komputer yang paling dominan dan didukung oleh hampir seluruh vendor komputer saat ini. Protokol inilah yang memungkinkan adanya internet.

2.2 JARINGAN KOMPUTER

Jaringan komputer dengan menggunakan server linux mampu mengelola semua servis internet, antara lain : router, database server, proxy server dan FTP server. Desain jaringan komputer berbasis klien server dengan server menggunakan sistem operasi linux dan klien windows dapat dilihat sebagai berikut :



Gambar 2.1
Jaringan Umum Komputer

Pada konfigurasi diatas server linux berfungsi sebagai database server dan juga sebagai router. Server linux memiliki 2 ethernet card, ethernet card 1 menggunakan nomor IP publik sedangkan ethernet card 2 menggunakan IP lokal. Komputer klien juga menggunakan IP lokal dan menjadi satu jaringan dengan server. Agar klien dapat mengakses internet maka server menggunakan perannya sebagai router untuk mem-forward IP masing-masing klien.

2.3 LINUX

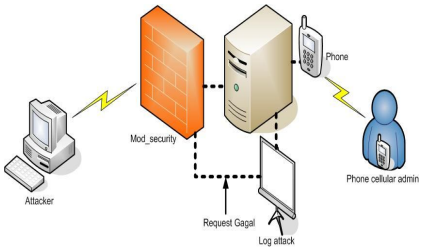
Linux adalah sebuah nama Operating System (OS) yang dibuat oleh Linus Trovalds dan didesain untuk dapat bekerja secara multitasking dan multiuser pada PC, dalam artian Linux mampu untuk menjalankan beberapa aplikasi secara bersamaan dan mendukung penggunaan aplikasi dan komputer untuk melayani beberapa pengguna sekaligus. Linux merupakan clone dari UNIX yang dapat bekerja pada PC, sehingga Linux memiliki kemampuan yang dimiliki oleh OS UNIX seperti :

- Multitasking dan multiuser, yaitu kemampuan untuk mnggunakan beberapa aplikasi secara bersamaan dan dapat melayani beberapa pengguna sekaligus.
- Mendukung implementasi jaringan dengan protocol TCP/IP. Protocol ini yang digunakan untuk melakukan komunikasi pada Jaringan (network).
- Virtual Memory. Memungkinkan penggunaan space harddisk sebagai memory.
- Shared Library. Memungkinkan penggunaan library secara bersama sehingga file executable lebih sedikit menggunakan ruang pada harddisk.
- Demand paged Loading. Hal ini akan memastikan hanya segment dari program yang benar-benar digunakan yang akan dibaca dari disk ke memory.
- Implementasi unified memory pool untuk program dan disk cache, sehingga semua free-memory akan digunakan untuk mempercepat proses.
- Dan satu yang menjadi kelebihan dari Linux adalah Linux murah (freeware) dibanding dengan UNIX, tetapi memiliki kemampuan hampir yang sama dengan UNIX.

BAB 3
PERENCANAAN DAN PEMBUATAN

3.1 GAMBARAN GLOBAL

Secara teknis proyek akhir ini membahas tentang security pada server web dengan menggunakan bantuan modul apahe yaitu *mod_security.*



Gambar 3.1 Blok diagram global

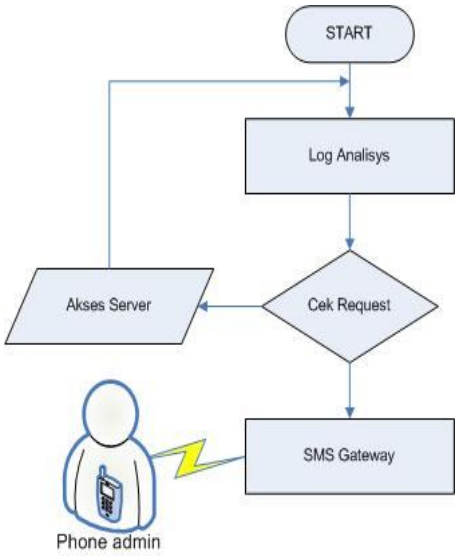
Keterangan :

User dalam suatu jaringan Lan/Internet ketika request suatu halaman web akan melewati firewall/security. Disini

pertama – tama mod_security akan memeriksa request yang datang. Pemeriksaan ini termasuk ip address user, user agent, jenis file yang direquest, serta inputan yang diinputkan pada web server. Request tersebut kembali diperiksa apakan objek yang diminta dianggap berbahaya atau tidak oleh firewall/security yang ada. Jika request yang di minta dianggap membahayakan maka akan didrop/ditolak dan semua informasi mengenai user akan di simpan pada log file yang telah di sediakan. Tetap jika request tersebut dianggap tidak membahayakan maka akan diijinkan untuk mengaksess halaman yang di minta.

3.2 PERENCANAAN PROGRAM

Semua user yang mengakses web server akan mengalami proses penyadapan infomasi dengan adanya aplikasi mod_security yang dijalankan oleh admin. Adapun diagram alir dari proses penyadapan informasi secara umum adalah sebagai berikut :



Gambar 3.2
Flowchart System Firewall

Aplikasi firewall yang terdapat pada sisi admin berlaku untuk semua user yang berada dimanapun baik dari sisi admin/localhost dan semua user/anonymous yang mengakses server web.

BAB 4
PENGUJIAN HASIL DAN ANALISA

4.1 PENGUJIAN SISTEM

Pada bab ini dimaksudkan untuk mengetahui keseluruhan pengujian dari perencanaan hasil dari system yang telah dibuat. Dengan demikian akan diketahui tingkat keberhasilan dari system yang telah dibuat. Pengujian yang dilakukan meliputi:

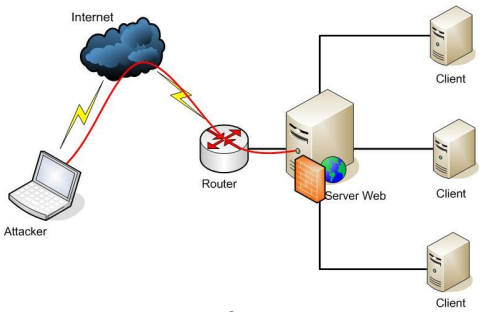
- Pengujian dan analisa penyerangan system firewall (mod_security) pada jaringan.
- Teknik serangan menggunakan SQL Injection.

4.2 Pengujian dan Analisa Penyerangan system firewall

Pada percobaan ini akan dilakukan penyerangan terhadap sistem firewall mod_security dari jaringan yang berbeda.

4.2.1 Pengujian menggunakan SQL Injection

Pada proyek akhir ini, untuk mengetahui berhasil atau tidaknya sistem firewall yang dibuat, ditentukan dari kemampuan sistem untuk memblokir dan mencatat serangan ke logfile. Pengujian dilakukan dengan mengadakan serangan dari jaringan yang berbeda, yaitu dengan menggunakan teknik SQL Injection. Skenario penyerangan yang akan dilakukan adalah sebagai berikut:



Gambar 4.1
Serangan dari luar/internet

Pada percobaan ini adalah dengan mengadakan usaha injection script SQL Injection pada web server dari jaringan luar/internet dengan teknik SQL Injection.

BAB 5
PENUTUP

Setelah dilakukan pengujian alat, maka diperoleh beberapa kesimpulan dan saran yang diharapkan berguna untuk pengembangan ilmu pengetahuan dan teknologi serta bagi kelanjutan dalam penyempurnaan system ini.

5.1 KESIMPULAN

Berdasarkan studi dan penelitian yang telah dilakukan pada bab sebelumnya, maka dapat disimpulkan beberapa hal antara lain:

- Tiap intrusi yang diinjekkan menghasilkan log file yang berbeda - beda.
- System firewall dapat mendeteksi serangan hacker yang menggunakan teknik SQL Injection.
- Hasil dari penditeksian seragan dapat ditampilkan dan dikirim melalui media sms.
- Dari pengujian tugas akhir ini menunjukkan bahwa tidak ada system firewall yang 100% solid.

5.2 SARAN

Saran – saran yang dapat dipertimbangkan untuk pengembangan pada proyek akhir di masa mendatang :

- Berbagai jenis serangan/tindakan hacking perlu diujicobakan, agar dihasilkan system firewall yang benar – benar solid.
- Implementasi system firewall yang layak ditanamkan pada server – server website, diutamakan untuk server – server web hosting.

DAFTAR PUSTAKA

[1] Kadir, Abdul., "Dasar Pemrogaman Web Dinamis Menggunakan PHP", Penerbit ANDI, Yogyakarta 2003.

[2] http://lirva32.org, "Lindungi Asset Web Server Dengan Mode Security" , 2008.

[3] http://www.modsecurity.org, "Mod_Security Reference Manual", 2008.

[4] http://isp-control.net, "[HowTo] Mod Security on debian", 2007.

[5] http://www.somacon.com, "Perl Regular Expresion", 2009.

[6] http://www.wellho.net, "Regular Expresion", 2008.